Policy 7 changes

Section 4: Filing- An employee may file a written grievance with his or her immediate supervisor within five (5) days after the occurrence of the event being grieved, or within (5) days after becoming aware of the event. The grievance statement must be submitted to the supervisor in writing, and it should state the specific claim and the specific relief desired.

Section 5: Steps- The employee grievance procedures provide for a minimum of two (2) steps for covered and handicapped employees who do not report directly to their department heads. Generally, the immediate supervisor will hear the grievance in the first step and the department head will hear the grievance in the second step.

Section 6: Scheduling and Notification- If the claim is determined to be grievable by the County Manager, the first hearing should be held within five (5) days after the grievance is filed. The immediate supervisor should notify the grievant of his or her decision in writing within three (3) days of the hearing. If the grievant is entitled to have a second hearing, he or she should notify the department head within five (5) days after receiving the initial decision. The department head should schedule the second hearing within five (5) days of receiving the request. If there is a second hearing, the department head should notify the grievant of his or her decision within three (3) days of the hearing.

Section 10: Appeal- An appeal is a request for a formal review of personnel action or decision made to the Department Head and County Manager.

Section 11: Procedure to Appeal Adverse Actions - The employee must present a written appeal request to their Department Head within five (5) work days of when the adverse action was issued to the employee. The Department Head issue a written decision supporting, reversing, or modifying the adverse action to the employee within five (5) work days of receipt of the written request for review. The written decision shall also notify the employee of the employee's right to appeal (if any) in accordance with the County's Appeal procedure. The written decision shall be provided to the employee and placed in the employee's personnel record.

If the employee is dissatisfied with the decision of the Department Head, The employee may request that the adverse action be reviewed by the County Manager. The employee must present a written request to the County Manager within five (5) work days of receipt of the written decision of the Department Head. The County Manager shall review all the documentation surrounding the adverse action and render a written decision supporting, reversing, or modifying the adverse action within five (5) work days of receipt of the written request for review. The written decision of the County Manager will be the final decision in the appeal process. Any further action taken by the employee must be through civil court proceedings. The written decision shall be provided to the employee and placed in the employee's personnel record.

Section 12: Procedure to Appeal Adverse Actions, Supervisory Personnel - This appeal procedure shall be followed as described above except that when the employee at issue is a Department Head the appeal process shall be amended accordingly.

Where the employee is a Department head the appeal procedure shall consist of a meeting with or review by the County Manager.

Section 13: Adverse Actions as Part of Employee's Personnel File - Documentation from adverse actions shall be placed in and become part of the employee's personnel file.

Section 14: Meeting and Response Time Frames - Notwithstanding any provisions in this policy to the contrary, should any meeting or response time frame contemplated herein involving the Department Head or County Manager conflict with the Department Head's or County Manager's ability to accomplish same, the Department Head or County Manager, as the case may be, shall notify the employee in writing of the inability to meet the meeting or response time frame and the reason therefore. This written notification shall be mailed to the employee's home address. The Department Head or County Manager, as the case may be, shall provide an alternate meeting date or response date within the aforementioned written notification.

Section 15: Emergency Action - The County Manager and/or Department Head may take immediate action against an employee under emergency situations. The immediate action will be to place the employee on administrative leave until an investigation can be conducted. If discipline is appropriate, the foregoing disciplinary procedures will be followed. Examples of emergency situations include crimes of moral turpitude, commission of a felony, injurious or dangerous behavior, and damage to or destruction of public property.

Leave Policy Change Recommendations

Policy 4 – ATTENDANCE AND LEAVE

Section 2: Donation of ~~Vacation~~ Annual/Sick ~~Time~~ Leave- When an employee is under the care of a physician, is unable to return to work, and has exhausted all their accrued sick and annual leave, accrued ~~vacation~~ annual or sick ~~time~~ leave may be donated to them by another employee as an exception to policy.

An employee who desires to donate accrued leave must make a request in writing through their supervisor to the County Manager. An employee who desires to donate, must maintain a minimum of forty (40) hours of accrued leave after the donation. ~~The donation must be equal or greater value than the cost of the salary and benefits being paid to the employee who will receive it~~. If approved, adjustments will be made to both employees' pay records.

Section 22: Family and Medical Leave- The Family and Medical Leave Act is intended to provide employees with the option of taking leave, due to an illness, family illness (Spouse, child or parent, birth of a child, adopted or foster child, surgery, etc.) without pay for a maximum period of twelve (12) weeks. The county will afford employees all rights under the Act in accordance with the Act's guidelines for employers. All duties imposed upon employees and the county, including exceptions, apply even if not stated in this policy.

Employees who have been employed for at least one (1) year and for at least 1,250 hours during the preceding 12-month period are eligible for family and medical leave, not to exceed twelve (12) weeks. ~~If leave is requested for any qualified medical reason, the employee must first use all of his or her accrued annual leave, compensatory time, and sick leave. If leave is requested for any other qualified reason, the employee must first use all of his or her accrued annual leave and compensatory time. The remainder of the twelve-week period will then consist of unpaid leave.~~ Employees will be required to apply all paid and unpaid leave concurrent with FMLA leave. Employees will not accrue additional paid leave while utilizing FMLA leave except leave which is donated to them. Employees receiving pay for the use of paid leave will be required to comply with all of the requirements of Ben Hill County's paid leave policies. An employee's accrued leave and/or workers' compensation will not be applied towards FMLA leave if the employee is taking FMLA leave for any purpose other than that allowed under those policies and provided further that an employee will not be required to take paid leave concurrent with FMLA leave if the employee is receiving income benefits under workers' compensation law.

Acceptable Use Policy

This acceptable use policy is written for Ben Hill County (Company). It is to be signed by all active employees and kept in their personnel file. This policy may be modified or updated at any time.

1. **Overview**

   Company provides access to information technology resources, including computers, networks, and peripheral devices as well as cloud services, SaaS platforms, identity systems, and remote access tools, to support the Company mission.

   These resources include, but are not limited to:

   - Cloud platforms (e.g., Microsoft 365, Google Workspace)
   - Identity providers and authentication systems
   - Remote access and zero trust solutions
   - Mobile and endpoint-managed devices
   - AI-powered tools and services

   Company is committed to protecting Company's employees, partners, and Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

   Internet/Intranet/Extranet-related systems, **including, but not limited to,** computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of the Company. These systems are to be used for business purposes in serving the interests of the Company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

   Effective security is a team effort involving the participation and support of every Company employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. **Purpose**

   The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at the Company. These rules are in place to protect the employee and Company. Inappropriate use exposes the Company to cyber risks including, but not limited to, virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

3. **Scope**

This policy applies to the use of information, electronic and computing devices, and network resources including cloud-based systems and third-party hosted services. All employees, contractors, consultants, temporary, and other workers at the Company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Company policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Company, including all personnel affiliated with third parties. This policy applies regardless of:

- Device ownership (Company-owned, personal, or third-party)
- Location (on-site, remote, or hybrid work environments)
- Network (corporate, home, public WiFi, or mobile networks)

4. Policy

4.1 General Use and Ownership

4.1.1 Company proprietary information stored on electronic and computing devices whether owned, leased or subscribed to by the Company, employee or a third party, remains the sole property of the Company. You must ensure that all proprietary information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of any Company proprietary information.

4.1.3 You may access, use or share Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within the Company or authorized third parties may monitor equipment, systems, and network traffic at any time.

4.1.6 Company reserves the right to audit networks and systems to ensure compliance with this policy.

4.1.7 Company data may reside in cloud systems and must be handled with the same level of protection as on-premises systems.

4.1.8 Users should assume that all activity conducted on Company systems, including cloud platforms, is logged and subject to monitoring.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy (Appendix A)*.

4.2.2 System level and user level passwords must comply with the Password Policy (Appendix B). All users must utilize Multi-Factor Authentication (MFA) where available. MFA is required for:

- Email systems
- Remote access
- Administrative accounts
- Cloud services

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended. Devices must also:

- Be encrypted
- Run Company-approved endpoint protection
- Receive regular updates and patches

4.2.4 Postings by employees from a Company email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is part of their Company business duties.

4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.2.6 Users must:

- Treat all unexpected emails, attachments, and links as suspicious
- Never trust emails containing passwords or urgent requests without verification
- Verify requests through a secondary trusted communication method

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities.

Under no circumstances is an employee of Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Company owned, leased, or subscribed to resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Company business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Company account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior approval is received from the Company.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Company network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Company employees to parties outside the Company.
18. Connecting personal devices, otherwise known as Bring Your Own Device (BYOD), and/or unauthorized devices to the Company network is strictly prohibited. Personal devices (BYOD) may only connect to Company systems if:
    - Approved by the Company
    - Managed or secured according to Company standards
    - Enrolled in endpoint or mobile device management (MDM), where applicable

4.3.2 Email and Communication Activities

When using Company resources to access and use the Internet, users must realize they represent the company. Whenever employees state

an affiliation to the Company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Company.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Company or connected via Company's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Limited personal email use may be permitted if it does not:
    - Interfere with work responsibilities
    - Introduce security risks
    - Violate Company policies

4.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by employees, whether using the Company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Use of the Company's systems to engage in blogging or other online posting related to the employees job duties is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Company's policy, is not detrimental to the Company's best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from the Company's systems is also subject to monitoring.
2. Company's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other

material covered by Company's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Company and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
4. Employees may also not attribute personal statements, opinions or beliefs to the Company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of the Company. Employees assume any and all risks associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the Company's trademarks, logos and any other Company intellectual property may also not be used in connection with any blogging or social media activity.
6. Limited personal social media use is permitted if:
    - It does not interfere with work duties
    - It does not expose Company systems to risk
    - It complies with Company conduct standards

4.4 Cloud and Data Handling

4.4.1 Company data must only be stored in approved systems.

4.4.2 Unauthorized use of personal cloud storage (Dropbox, Google Drive personal, etc.) is prohibited.

4.4.3 Sharing Company data externally must follow Company-approved methods.

4.4.4 Public sharing links must be restricted and time-limited where possible.

4.4.5 Sensitive data must not be downloaded to unmanaged devices.

4.5 Remote Work and Network Use

4.5.1 Users must secure home networks with:

- Strong WiFi passwords
- Updated firmware

4.5.2 Public WiFi use must be avoided unless using Company-approved secure access (VPN or Zero Trust).

4.5.3 Devices must not be left unattended in unsecured environments.

4.6 Acceptable Use of Artificial Intelligence (AI)

The use of AI tools (e.g., ChatGPT, Microsoft Copilot, Google Gemini, or similar platforms) introduces new risks related to data exposure, accuracy, and compliance. Employees must adhere to the following guidelines:

4.6.1 Approved Use

- AI tools may be used to improve productivity, research, drafting, and problem-solving.
- AI-generated content must always be reviewed for accuracy and appropriateness.

4.6.2 Prohibited Use

Employees must NOT:

- Input confidential, sensitive, or non-public Company data into AI tools
- Input client data, personally identifiable information (PII), or protected data
- Use AI tools to bypass security controls or policies
- Rely solely on AI-generated output without validation

4.6.3 Data Protection

- Assume anything entered into an AI tool may be stored or used for training
- Do not upload:
  - Internal documents
  - Financial data
  - Credentials or system configurations
  - Legal or HR information

4.6.4 Output Responsibility

- Employees are responsible for all AI-assisted work
- AI output must not be treated as authoritative without verification
- Any decisions impacting operations, security, or customers must be validated

4.6.5 Shadow AI

- Use of unapproved AI tools or browser extensions is prohibited
- Only Company-approved AI tools may be used for business purposes

4.6.6 Compliance

AI use must comply with:

- Data protection laws
- Industry regulations
- Company confidentiality policies

5. Policy Compliance

5.1 Compliance Measurement

Company will verify compliance to this policy through various methods including, but not limited to, business tool reports, internal and external audits, and feedback by the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Company in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix A - Minimum Access Policy

The Company employs the principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) which requires that every process, program, or user must only be able to access the information and resources that are absolutely necessary. This minimizes the level of access to files and directories that may contain sensitive information.

1. **Scope**
   This policy applies to employees, contractors, consultants, temporaries, and other workers at Company, including all personnel affiliated with third parties.

2. **Procedure**
   File System Security - the Company provides minimum access to files and directories. No user should attempt to access files or directories unless they are explicitly authorized to do so.

   Computer Network Connection - Users may only connect to the Company network using only equipment that is owned, leased or subscribed to by the Company.

3. **Enforcement**
   Violation of this procedure could be grounds for disciplinary action up to and including termination.

Appendix B - Password Policy

1. **Overview**

   Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorized access to the most sensitive data and/or exploitation of Company resources. All employees, contractors, consultants, temporaries, other workers, and all personnel affiliated with third parties with access to Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. **Purpose**

   The purpose of this policy is to establish a standard for the secure use and protection of all work related passwords.

3. **Scope**

   The scope of this policy includes all personnel who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any Company facility, has access to the Company network, or stores any non-public Company information.

4. **Policy**

   4.1 Password Creation and Use

   4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines (Appendix C).*

   4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

   4.1.3 Staff will be provided password management tools to securely store and manage all their work related passwords. In the event a password management tool is not provided by the Company, staff are allowed to use a password management tool from a list of approved password management tools to securely store and manage all of their work related passwords. In the event a staff member uses a password management tool not provided by the Company, staff member acknowledges after a separation from employment for any reason that the staff member MUST SECURELY DELETE all work related passwords and user account information from the password management tool.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs, such as "sudo", must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2 Password Change

4.2.1 Passwords should be changed upon expiration, when there is reason to believe a password has been compromised, or if the password fails to meet the Company's Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Company information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in password managers provided or approved by the Company.

4.3.4 Passwords should never be stored anywhere in plain text. Examples of storing passwords in plain text include, but are not limited to, writing them in a notebook, writing them on a sticky note or saving them in unencrypted files on a computer such as a text file or spreadsheet.

4.3.5 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.6 Any individual suspecting that their password may have been compromised must report the incident immediately and change all relevant passwords.

4.4 Multi-Factor Authentication

4.4.1 Multi-factor authentication is **required** for all supported systems and accounts.

5. Policy Compliance

5.1 Compliance Measurement

Company will verify compliance to this policy through various methods including, but not limited to, business tool reports, and internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by the Company.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix C - Password Construction Guidelines

1. **Overview**

   Passwords are a critical component of information security. Passwords serve to protect access to user accounts, data and systems. However, a poorly constructed or easily guessed password can compromise the strongest defenses. This guideline provides best practices for creating strong passwords.

2. **Purpose**

   The purpose of this guideline is to provide best practices for the creation of strong passwords.

3. **Scope**

   This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including, but not limited to, user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and local router logins.

4. **Policy**

   Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of 16 characters in all work related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include "It's time for vacation" or "block-curious-sunny-leaves". Passphrases are both easy to remember and type, yet meet the strength requirements of a strong password.

   Password cracking or guessing may be performed on a periodic or random basis by Company or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change that password immediately.

5. **Policy Compliance**

   5.1 Compliance Measurement

   Company will verify compliance to this policy through various methods, including but not limited to, business tool reports, and internal and external audits.

   5.2 Exceptions

   Any exception to the policy must be approved by the Company.

   5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

POLICY 12

INTERNET & ELECTRONIC COMMUNICATON

Section 1: Policy Statement- Use of County computers, networks, email, Internet access, cloud services, mobile devices, remote access systems, AI tools, and related technology resources is governed by the Ben Hill County Acceptable Use Policy, as adopted and amended from time to time. While personal electronic devices are allowed in the workplace, their use should be limited to breaks and lunch periods. The County expects these devices to be used responsibly, similar to using a workplace County phone.

Section 2: Relationship to Other Policies- Relationship to Other Policies-The Acceptable Use Policy supplements all Ben Hill County policies relating to workplace harassment, discrimination, retaliation, conflicts of interest, discipline and discharge, records retention, and Open Records/Open Meetings Act compliance.

Section 3: No Expectation of Privacy- Employees have no expectation of privacy when using County technology resources, including computers, email, networks, cloud systems, remote access tools, mobile devices, and other County-provided or County-managed systems. Authorized County personnel or authorized third parties may monitor, access, audit, and review systems, data, and network activity as permitted by law and County policy.

Section 4: Public Records- Many emails and other electronic files constitute public records for purposes of state record retention laws and Georgia's Open Records Act. As such, whether a given email or electronic file is subject to a retention schedule must be determined by its content rather than its format. As a general rule, any email or other electronic file which is a substitute for a letter, memorandum, notice, report, or other traditional record that would be subject to a particular retention schedule, then it too is subject to the schedule. Conversely, if the email or other electronic file is merely transitory, it need not be retained beyond its useful life (e.g., listserv messages, meeting notices, general staff announcements, invitations to events, etc.). Users of Ben Hill County computers and other computer-related services must also bear in mind that all emails and other electronic files may be subject to disclosure under the Open Records Act.

Section 5: Acceptable Uses- Acceptable uses of County technology resources are governed by the Ben Hill County Acceptable Use Policy.

Section 6: Specifically Unacceptable Uses- Prohibited and restricted uses of County technology resources are governed by the Ben Hill County Acceptable Use Policy and related County conduct, harassment, discrimination, retaliation, confidentiality, and records policies.

Section 7: Procedures- Department Heads, supervisors, and authorized IT personnel are responsible for supporting compliance with the Acceptable Use Policy. Access to County systems may be suspended, limited, or withdrawn when necessary to protect the security,

operation, or integrity of County systems. Violations may result in disciplinary action, up to and including termination, and may be referred for civil or criminal action when applicable.

Section 8: Guidelines- The following additional guidelines apply to uses of the Internet and email made available to employees by Ben Hill County:

(a) Correspondence with Legal Counsel/Disclaimer - Any email or other correspondence sent to the County Attorney or other legal counsel for Ben Hill County, if sent for the purpose of assisting legal counsel in providing legal advice to Ben Hill County, must include the following disclaimer; **"This communication and all attachments may contain privileged and confidential legal communications/attorney work product intended solely for the use of the addressee. If you are not the intended recipient, any reading, distribution, copying or other use of this communication and/or any attachments hereto is prohibited and you should delete this message from all locations, and advise the sender at [INSERT TELEPHONE NUMBER AND/OR EMAIL ADDRESS]. Thank you."**

Section 9: Use of Computer Software- Use of Computer Software- Software use, installation, copying, and licensing compliance are governed by the Acceptable Use Policy. Employees may not install, copy, download, or use software except as authorized by the County and permitted by applicable license terms.

POLICY 13

EMPLOYEE INTRANET AND SOCIAL MEDIA

Section 1: Policy- The purpose of this policy is to establish guidelines for employees who post information to and access personal web pages or social networking technologies. Ben Hill County, through this policy, seeks to establish some basic guidelines for county employees who use social media technologies, both at the worksite and away from it. The intent of this policy is not to prohibit employees' personal expression on the Internet. Ben Hill County reaffirms its commitment to freedom of speech as guaranteed by the First Amendment to the U.S. Constitution. Accordingly, nothing in this Employee Intranet and Social Media Policy is intended to limit any speech or conduct protected by the First Amendment. However, an employee's online presence reflects upon the County, and employees should be aware that actions captured via images, posts, or comments may discredit the County or adversely affect the efficiency or integrity of the County.

Limited personal social media use is permitted only as allowed by the Acceptable Use Policy and only when it does not interfere with work duties, expose County systems to risk, or violate County conduct standards.

Section 2: Scope- This Employee Intranet and Social Media Policy shall apply to all Ben Hill County personnel. This Employee Intranet and Social Media Policy applies to an employee's use

of social media technologies, both at the worksite (when authorized) during business hours and away from the worksite during non-business hours. Personnel who violate this Employee Intranet and Social Media Policy may be subject to disciplinary action, up to and including termination of employment.

Section 3: Definition & Applicability- Social media includes Internet-based or app-based platforms that allow users to create, share, post, comment on, stream, or exchange text, images, audio, video, or other content, including blogs, message boards, social networking sites, video-sharing platforms, messaging platforms, and similar technologies.

Section 4: Privacy- Ben Hill County employees should be aware that information posted on the Internet is not secure or private, even if active steps are taken to restrict access to an employee's site. Once information has been posted on the Internet, it is generally traceable and accessible indefinitely. In addition, law enforcement employees, in particular, are advised that, in the event information has been posted on the Internet identifying them as a law enforcement officer, they may be ineligible for specialized positions in which anonymity is required.

Section 5: Liability- All employees should be aware that due to the nature of their employment in the public sector, they are held to a higher standard. As a result, certain kinds of Internet postings may be detrimental in both the employee's personal and professional capacity. Whether social media technologies are used during or after business hours or posts made on personal or publicly accessible websites, employees are at all times representing Ben Hill County, and employee postings, images, etc. are a reflection of both the County and its staff. In the event employees choose to post information that is in violation of this Employee Intranet and Social Media Policy, they should be aware that they will be held accountable through the County's standards of conduct and action may be taken as outlined above. Employees should consider the possible adverse consequences of some Internet postings with respect to future employment, cross-examination in court cases, and potential public/private embarrassment. Employees are encouraged to seek the guidance of supervisors regarding any posting that they are concerned may adversely reflect upon either the County or upon the professionalism or integrity of the employee.

Section 6: Restrictions-

(a) General Use - Employees may post personal information that is not inconsistent with this or any other County policy. Such posts may include generally known and available information about County activities, including information about the workplace, an employee's projects, etc. for certain positions; the County recognizes social media as a significant and effective communication tool. General use of Social Media is governed by the Acceptable Use Policy.

(b) Co-Worker Interactions - Employees may be "friends' of other employees, at each employee's discretion. No employee is obligated, however, to interact with co-workers

through social media technologies. Supervisors are discouraged from being "friends" with subordinates.

(c) Photographs - If otherwise compliant with copyright and other legal restrictions, employees may post photographs or other depictions of Ben Hill County, including public areas of County facilities, events, etc. Employees may not post any photographs or other depictions of non-public work areas, employees, sensitive operations, incidents, equipment, records, or images with the express approval of their supervisor.

(d) Logos & Trademarks - Employees may not post the County's adopted logos and trademarks without written approval of the County Manager.

(e) Respect - Demonstrate respect for the dignity of the County, its citizens, its customers, its vendors, and its employees. Internet postings or messages left on social media sites are available for public viewing, and employees are encouraged to avoid embarrassing, harassing, or bullying other users of such sites, as well as County employees, customers, vendors, or citizens. You are encouraged to refrain from using ethnic slurs, personal insults, or obscenity, or using language that may be considered hateful or bullying. Even if a message is posted anonymously, it may be possible to trace it back to the sender.

(f) Post disclaimers - If an employee identifies himself or herself as a County employee or discusses matters related to the County on a website, web log, or social media site, the employee's web log or social media site must include a disclaimer on the front page stating that it does not express the views of the County and that the employee is expressing only his or her personal views. For example: "the views expressed on this website/weblog are mine alone and do not necessarily reflect the views of my employer." Place the disclaimer in a prominent position and repeat it for each posting expressing an opinion related to the County or the County's business. Employees must keep in mind that if they post information on a web log or social media site that is a violation of County policy and/or federal, state, or local law, the disclaimer will not shield them from disciplinary action.

(g) Worksite Usage - Personal social media use during working time is limited to the extent permitted by the Acceptable Use Policy and must not interfere with work duties, expose County systems to risk, or violate County policy. Social media use is permitted when directly related and necessary to perform assigned job duties.

(h) Files from County Devices - Employees may not upload any audio/video files or other data files captured on devices owned by Ben Hill County, without prior approval by his/her department manager.

(i) Political Communications and Participation - Employees are not permitted to use social media technologies to influence or affect the results of any election or nomination while acting in their official County capacity, on County time, or using any County equipment.

(j) Privileged & Confidential Information - Employees are not permitted to post any privileged or confidential information.

(k) Judgment - Employees should use good judgment in their postings and social media activity. If the content of a post is not something that an employee would feel comfortable with their supervisor reading or viewing, it is probably inappropriate and may conflict with this policy.

(l) "Likes"; "Retweets" - Use equal caution when "liking", sharing, or re-tweeting posts on social media to ensure compliance with this policy.